

Method and circuit arrangement for the distribution of keys on key devices.

Patent Number: EP0067977

Publication date: 1982-12-29

Inventor(s): RAUCH WALTER DIPL-ING; GRENZEBACH KURT; THENERT HELMUT

Applicant(s):: SIEMENS AG (DE)

Requested Patent: DE3123167

Application Number: EP19820104668 19820527

Priority Number(s): DE19813123167 19810611

IPC Classification: H04L9/02 ; H04K1/02

EC Classification: H04L9/08

Equivalents: NO821925

Abstract

For the coded transmission of messages between terminals (DE1, DE2) via a communication network, corresponding keys (S) are transmitted from a key distribution centre (SVZ) to the key devices (SG) via the communication network itself. The key distribution centre (SVZ) generates a data field (DF) which is provided with a key identification (SK), key device identifications (GK) allocated to the key devices and with key fields (SF). The key fields (SF) contain the actual keys (S), check characters (P) and other characters which define the time of validity of the key (S1). After the recognition of the key identification (SK) and the corresponding key device identification (GK), the corresponding keys (S) are stored in the key devices.



Data supplied from the esp@cenet database - I2

⑯ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑯ Patentschrift
⑯ DE 3123167 C1

⑮ Int. Cl. 3:
H 04 K 1/00

⑯ Aktenzeichen: P 31 23 167 5-35
⑯ Anmeldetag: 11. 6. 81
⑯ Offenlegungstag: —
⑯ Veröffentlichungstag: 24. 2. 83

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

⑯ Patentinhaber:

Siemens AG, 1000 Berlin und 8000 München, DE

⑯ Erfinder:

Rauch, Walter, Dipl.-Ing., 8027 Neuried, DE; Grenzebach,
Kurt, 6440 Bebra, DE; Thenert, Helmut, 6431 Heringen, DE

⑯ Entgegenhaltungen:

US 41 82 933

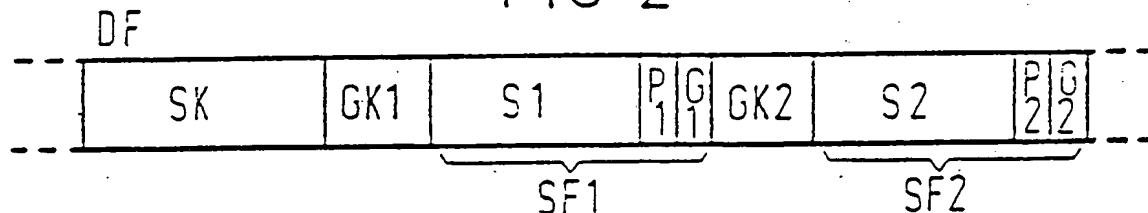
EP 23 074 A

⑯ Verfahren und Schaltungsanordnung zum Verteilen von Schlüsseln an Schlüsselgeräte

Zur verschlüsselten Übertragung von Nachrichten zwischen Endeinrichtungen (DE1, DE2) über ein Nachrichtennetz werden von einer Schlüsselverteilzentrale (SVZ) entsprechende Schlüssel (S) an die Schlüsselgeräte (SG) über das Nachrichtennetz selbst übertragen. Die Schlüsselverteilzentrale (SVZ) erzeugt ein Datenfeld (DF), das mit einer Schlüsselkennung (SK), den Schlüsselgeräten zugeordneten Schlüsselgeräte-

kennungen (GK) und Schlüsselfeldern (SF) versehen ist. Die Schlüsselfelder (SF) enthalten die eigentlichen Schlüssel (S), Prüfzeichen (P) und weitere Zeichen, die den Gültigkeitszeitpunkt des Schlüssels (S1) festlegen. Nach dem Erkennen der Schlüsselkennung (SK) und der entsprechenden Schlüsselgerätekennung (GK) werden in den Schlüsselgeräten die entsprechenden Schlüssel (S) eingespeichert. (31 23 167)

FIG 2



BEST AVAILABLE COPY

Patentansprüche:

1. Verfahren zum Verteilen von Schlüsseln an Schlüsselgeräte, die an einem Nachrichtennetz angeschlossen sind, und die unter Verwendung von einer Schlüsselverteilzentrale verteilten Schlüsseln über das Nachrichtennetz zu übertragende Nachrichten verschlüsseln, gekennzeichnet durch folgende Verfahrensschritte

- a) die Schlüsselverteilzentrale (SVZ) bildet einen Datenblock, der in einem Datenfeld (DF) eine Schlüsselkennung (SK), mindestens eine, einem Schlüsselgerät (SG) zugeordnete Schlüsselgeräterkennung (GK) und mindestens einen zugehörigen Schlüssel (S) enthält
- b) der Datenblock wird in entsprechender Weise wie die zu übertragenden Nachrichten über das Nachrichtennetz zu den jeweiligen Schlüsselgeräten (SG) übertragen
- c) in den Schlüsselgeräten (SG) werden die Schlüsselkennung (SK) und die Schlüsselgeräterkennungen (GK) geprüft
- d) beim Erkennen der Schlüsselkennung (SK) und der, dem jeweiligen Schlüsselgerät (SG) zugeordneten Schlüsselgeräterkennung (GK) wird der zugehörige Schlüssel (S) im Schlüsselgerät (SG) gespeichert.

2. Verfahren nach Anspruch 1, bei dem in einem Streckenabschnitt des Nachrichtennetzes zwei Schlüsselgeräte angeordnet sind, dadurch gekennzeichnet, daß das Datenfeld (DF) neben der Schlüsselkennung (SK) zwei Schlüsselgeräterkennungen (GK 1, GK 2) und zwei Schlüsselfelder (SF 1, SF 2) enthält, die jeweils einem der beiden Schlüsselgeräte (SG 1, SG 2) zugeordnet sind.

3. Verfahren nach Anspruch 1, bei dem zwischen zwei Endeinrichtungen (DE 1, DE 2) eine Teilnehmer-Teilnehmer-Verschlüsselung erfolgt, dadurch gekennzeichnet, daß das Datenfeld (DF) neben der Schlüsselkennung (SK) nur eine einem Schlüsselgerät (SG) zugeordnete Schlüsselgeräterkennung (GK) und einen zugehörigen Schlüssel (S) enthält.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der zu einem Schlüsselgerät (SG) übertragene Schlüssel (S) jeweils mit einem dem Schlüsselgerät (SG) zugeordneten Stationsschlüssel verschlüsselt übertragen wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß das Schlüsselfeld (SF) Prüfzeichen (P) enthält.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß das Schlüsselfeld (SF) Zeichen (G) enthält, die den Gültigkeitszeitpunkt und/oder die Gültigkeitsdauer des zugehörigen Schlüssels (S) im entsprechenden Schlüsselgerät (SG) festlegen.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß das Datenfeld (DF) auf den Übertragungsstrecken (FL) verschlüsselt übertragen wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß das Nachrichtennetz als Paketvermittlungsnetz ausgebildet ist.

9. Schaltungsanordnung zur Durchführung des Verfahrens nach Anspruch 1, dadurch gekennzeich-

ne, daß die Schlüsselgeräte (SG) jeweils eine erste Auswertestufe (A 11, A 21), die beim Erkennen der Schlüsselkennung ein Steuersignal (ST 1, ST 2) erzeugt und eine zweite Auswertestufe (A 12, A 22) enthalten, die beim Vorliegen der Steuersignale (ST 1, ST 2) und beim Erkennen der Schlüsselgeräterkennung (GK 1, GK 2) ein Freigabesignal (F 1, F 2) erzeugt, mit dem ein Einspeichern des jeweiligen Schlüssels (S 1, S 2) in einen Speicher (SP 1, SP 2) freigegeben wird.

10. Schaltungsanordnung nach Anspruch 9, dadurch gekennzeichnet, daß die Schlüsselgerät (SG) eine Zeitstufe (Z 1, Z 2) enthält, die unter Verwendung der im Datenfeld (DF) enthaltenen Zeichen (G) den Gültigkeitszeitpunkt und/oder die Gültigkeitsdauer des jeweiligen Schlüssels (S) steuert.

Die Erfindung bezieht sich auf ein Verfahren zum Verteilen von Schlüsseln an Schlüsselgeräte, die an einem Nachrichtennetz angeschlossen sind, und die unter Verwendung von einer Schlüsselverteilzentrale verteilten Schlüsseln über das Nachrichtennetz zu übertragende Nachrichten verschlüsseln, sowie auf eine Schaltungsanordnung zur Durchführung des Verfahrens.

Es ist allgemein bekannt, daß zur Übertragung von verschlüsselten Nachrichten zwischen Endeinrichtungen in den Übertragungsweg zwischen den Endeinrichtungen Schlüsselgeräte eingeschaltet werden müssen. Diese werden jeweils zwischen den Endeinrichtungen und Übertragungseinheiten angeordnet. Auf der Sendeseite werden die von der Endeinrichtung abgegebenen Nachrichten mittels des Schlüsselgeräts verschlüsselt und unter Verwendung der Übertragungseinheit an eine Fernleitung abgegeben. Auf der Empfangsseite werden die mittels der dortigen Übertragungseinheit empfangenen Nachrichten unter Verwendung des empfangsseitigen Schlüsselgerätes entschlüsselt und an die empfangende Endeinrichtung abgegeben. Zwischen den Übertragungseinheiten können beispielsweise Standverbindungen, ein Durchschaltewählernetz oder ein Nachrichtennetz mit speichernden Netzknöpfen (Paketvermittlungsnetz) eingeschaltet sein. Beim Durchschaltewählernetz ist eine Teilnehmer-Teilnehmer-Verschlüsselung und bei einem Nachrichtennetz mit speichernden Netzknöpfen ist sowohl eine abschnittsweise Verschlüsselung als auch eine Teilnehmer-Teilnehmer-Verschlüsselung üblich.

Üblicherweise wird jedem Schlüsselgerät von einer Schlüsselverteilzentrale individuell ein Stationsschlüssel zugeordnet. Für eine aktuelle Übertragung von Nachrichten oder für einen bestimmten Zeitabschnitt erzeugt die Schlüsselverteilzentrale einen weiteren Schlüssel und sendet diesen Schlüssel, verschlüsselt mit dem jeweiligen Stationsschlüssel an das betreffende Schlüsselgerät. Dieser aktuelle Schlüssel gilt dann für die Übertragung der Nachrichten zwischen den Datenendeinrichtungen solange, bis die Schlüsselverteilzentrale einen neuen Schlüssel zuteilt.

Eine übliche, vielfach praktizierte Maßnahme ist die Verteilung der Schlüssel an die entsprechenden Schlüsselgeräte unter Verwendung von Datenträgern, wie beispielsweise Lochkarten, Lochstreifen oder magnetischen Datenträgern, die auf dem Postwege oder durch Kuriere verteilt werden. In Nachrichtensystemen,

in denen sehr viele Datenendeinrichtungen miteinander korrespondieren, ist eine derartige Schlüsselverteilung jedoch nicht mehr praktikabel.

Es wäre denkbar, neben dem Nachrichtennetz, an die die Schlüsselgerät über die Übertragungseinrichtungen angeschlossen sind, ein Schlüsselverteilnetz vorzusehen, über das den einzelnen Schlüsselgeräten die aktuellen Schlüssel auf elektronischem Wege zugeteilt werden. Eine derartige Schlüsselverteilung erfordert jedoch einen verhältnismäßig großen Aufwand.

Aus der US-PS 41 82 933 ist es bekannt, den einzelnen Schlüsselgeräten die aktuellen Schlüssel über das Nachrichtennetz zu übertragen, über das auch der Austausch der Nachrichten zwischen den Schlüsselgeräten erfolgt. An dem Nachrichtennetz ist eine Schlüsselverteilzentrale angeschlossen, die nach einer entsprechenden Aufforderung durch das rufende Schlüsselgerät den aktuellen Schlüssel auf elektronischem Wege dem sendenden Schlüsselgerät und gegebenenfalls auch dem empfangenden Schlüsselgerät mitteilt. Dieses Verfahren erfordert eine verhältnismäßig umfangreiche Prozedur und eine Mehrzahl von Übertragungen zwischen dem sendenden Schlüsselgerät und der Schlüsselverteilzentrale.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Schaltungsanordnung anzugeben, mit deren Hilfe auf einfache Weise und mit geringem Aufwand eine Verteilung von Schlüsseln an eine Mehrzahl von Schlüsselgeräten ermöglicht wird.

Erfnungsgemäß wird die Aufgabe bei dem Verfahren der eingangs genannten Art gelöst: durch die zeitliche Aufeinanderfolge folgender Verfahrensschritte:

- a) die Schlüsselverteilerzentrale bildet einen Datenblock, der in einem Datenfeld eine Schlüsselkennung, mindestens eine, einem Schlüsselgerät zugeordnete Schlüsselgerätekennung und mindestens einen zugehörigen Schlüssel enthält,
- b) der Datenblock wird in entsprechender Weise wie die zu übertragenden Nachrichten über das Nachrichtennetz zu den jeweiligen Schlüsselgeräten übertragen,
- c) in den Schlüsselgeräten werden die Schlüsselkennung und die Schlüsselgerätekennungen geprüft,
- d) beim Erkennen der Schlüsselkennung und der dem jeweiligen Schlüsselgerät zugeordneten Schlüsselgerätekennung wird der zugehörige Schlüssel im Schlüsselgerät gespeichert.

Das Verfahren gemäß der Erfindung hat den Vorteil, daß neben dem bestehenden Nachrichtennetz kein weiteres Netz erforderlich ist, und es damit einem äußerst geringen Aufwand erfordert. Für die Übertragung der Schlüssel können die normalen, auch für die Übertragung der Nachrichten vorgesehenen Prozeduren verwendet werden. Die Schlüsselgeräte müssen die für die Übertragung der Nachrichten vorgesehenen Prozeduren nicht kennen, und können daher sehr vielseitig eingesetzt werden. Außerdem erfordern die Schlüsselgeräte keine zusätzlichen, neu zu definierenden Schnittstellen.

Das Verfahren gemäß der Erfindung kann insbesondere dann in vorteilhafter Weise eingesetzt werden, wenn die Übertragung der Nachrichten über ein Nachrichtennetz mit speichernden Netzknoten erfolgt. Falls die Nachrichten abschnittsweise verschlüsselt übertragen werden, und in den einzelnen Streckenab-

schnitten des Nachrichtennetzes jeweils zwei Schlüsselgeräte angeordnet sind, ist es vorteilhaft, wenn das Datenfeld neben der Schlüsselkennung zwei Schlüsselgerätekennungen und zwei Schlüsselfelder enthält, die jeweils einem der beiden Schlüsselgeräte zugeordnet sind.

Falls die Übertragung der Nachrichten entsprechend einer Teilnehmer-Teilnehmer-Verschlüsselung erfolgt, und damit in einem, einer Datenendeinrichtung 10 zugeordneten Streckenabschnitt nur ein einziges Schlüsselgerät vorgesehen ist, ist es vorteilhaft, wenn das Datenfeld neben der Schlüsselkennung nur eine einem Schlüsselgerät zugeordnete Schlüsselgerätekennung und einen zugehörigen Schlüssel enthält.

Um den jeweils aktuellen Schlüssel noch innerhalb des Netzknotens verschlüsselt übertragen zu können, ist es zweckmäßig, wenn der zu einem Schlüsselgerät übertragene Schlüssel jeweils mit einem dem Schlüsselgerät zugeordneten Stationsschlüssel verschlüsselt 20 übertragen wird.

Zur Sicherung des aktuellen Schlüssels und/oder des gesamten Datenfeldes ist es vorteilhaft, wenn das Schlüsselfeld Prüfzeichen enthält.

Falls der neue Schlüssel nicht sofort in Kraft treten soll, ist es günstig, wenn das Schlüsselfeld Zeichen enthält, die den Gültigkeitszeitpunkt und/oder die Gültigkeitsdauer des zugehörigen Schlüssels im entsprechenden Schlüsselgerät festlegen.

Zur Sicherung des Datenfels auf den Streckenabschnitten ist es günstig, wenn das Datenfeld auf den Übertragungsstrecken verschlüsselt übertragen wird.

Eine besonders vorteilhafte Anwendung des Verfahrens wird erreicht, wenn das Nachrichtennetz als Paketvermittlungsnetz ausgebildet ist.

In diesem Fall ist das Datenfeld ein Block, der neben dem Datenfeld ein Adressfeld, ein Steuerfeld und ein Blockprüfungsfeld enthält.

Bei einer vorteilhaften Schaltungsanordnung zur Durchführung des Verfahrens wird das Datenfeld in der Schlüsselverteilerzentrale zusammengestellt und in ähnlicher Weise wie von einer Datenendeinrichtung an das Nachrichtennetz abgegeben. Zum Erkennen des jeweiligen Schlüssels im Schlüsselgerät ist es vorteilhaft, wenn die Schlüsselgeräte jeweils eine erste Auswertestufe, die 40 beim Erkennen der Schlüsselkennung ein Steuersignal erzeugt und eine zweite Auswertestufe enthalten, die beim Vorliegen der Steuersignale und beim Erkennen der Schlüsselgerätekennung ein Freigabesignal erzeugt, mit dem ein Einspeichern des jeweiligen Schlüssels in 45 einen Speicher freigegeben wird.

Für die Aktivierung des Schlüssels ist es günstig, wenn das Schlüsselgerät eine Zeitstufe enthält, die unter Verwendung der im Datenfeld enthaltenen Zeichen den Gültigkeitszeitpunkt und/oder die Gültigkeitsdauer des 55 jeweiligen Schlüssels steuert.

Im folgenden wird eine Durchführung des Verfahrens gemäß der Erfindung anhand von Zeichnungen näher erläutert. Es zeigt

Fig. 1 ein Blockschaltbild einer Übertragungsanordnung mit einem Nachrichtennetz mit speichernden Netzknoten.

Fig. 2 den Aufbau eines Datenfeldes in einem Datenblock,

Fig. 3 ein Blockschaltbild von Teilen von Schlüsselgeräten.

Bei dem in Fig. 1 dargestellten Nachrichtennetz mit speichernden Netzknoten NK (Paketvermittlungsnetz) wird angenommen, daß die Nachrichten, beispielsweise

Daten abschnittsweise verschlüsselt von einer Datenendeinrichtung DE_1 zu einer Datenendeinrichtung DE_3 übertragen werden. Die von der Datenendeinrichtung DE_1 abgegebenen Daten werden in einem Schlüsselgerät SG_1 verschlüsselt und über eine Datenübertragungseinheit DU_1 an eine Fernleitung FL_1 abgegeben. Eine Datenübertragungseinheit DU_2 empfängt die verschlüsselten Daten und gibt sie an ein Schlüsselgerät SG_2 ab. Dieses entschlüsselt die Daten und überträgt sie über den Netzknoten NK zu einem Schlüsselgerät SG_3 . Dieses verschlüsselt die Daten erneut und gibt sie über eine Datenübertragungseinheit DU_3 an eine Fernleitung FL_2 ab. An der Fernleitung FL_2 ist eine weitere Datenübertragungseinheit DU_4 angeschlossen, die die verschlüsselten Daten an ein Schlüsselgerät SG_4 abgibt. Dort werden sie wieder entschlüsselt und der Datenendeinrichtung DE_2 zugeführt.

Die Ver- und Entschlüsselung der Daten in den Schlüsselgeräten SG_1 bis SG_4 erfolgt unter Verwendung eines, jedem Schlüsselgerät individuell zugeordneten Stationsschlüssels und eines für den jeweils aktuellen Vorgang geltenden weiteren Schlüssels. Der Stationsschlüssel wird beispielsweise von Hand in das entsprechende Schlüsselgerät eingegeben. Eine Schlüsselzentrale SVZ kennt die jeweiligen Stationsschlüssel. Die jeweils für eine Übertragung von Daten geltenden aktuellen Schlüssel sind ebenfalls in der Schlüsselverteilzentrale SVZ bekannt und sie werden über das Nachrichtennetz an die an der Übertragung beteiligten Schlüsselgeräte verschlüsselt übertragen. Die Übertragung zu den Schlüsselgeräten erfolgt dabei in denselben Prozeduren, wie auch die übliche Übertragung von Nachrichten. Die Schlüsselverteilzentrale SVZ ist zum Zweck der Übertragung der Schlüssel in ähnlicher Weise wie die Datenendeinrichtungen DE_1 und DE_2 über ein Schlüsselgerät SG_5 , eine Datenübertragungseinheit DU_5 , gegebenenfalls eine Fernleitung FL_3 , eine weitere Datenübertragungseinheit DU_6 und ein weiteres Schlüsselgerät SG_6 an dem Netzknoten NK angeschlossen.

Bei der Zuteilung eines Schlüssels für eine abschnittsweise Verschlüsselung der Daten, erzeugt die Schlüsselverteilzentrale SVZ einen Datenblock, der in ähnlicher Weise aufgebaut ist, wie ein normaler Nachrichtenblock. Der Datenblock wird jedoch mit einer besonderen Adresse gekennzeichnet, so daß die zugeordnete Datenendeinrichtung den mit den Schlüsseln versehenen Block sofort erkennen kann.

Der in Fig. 2 dargestellte Ausschnitt aus einem Datenblock enthält ein Datenfeld DF , das mit Schlüsseln für die Schlüsselgeräte SG_1 und SG_2 versehen ist. Ein entsprechender Datenblock wird für die Übertragung der Schlüssel zu den Schlüsselgeräten SG_3 und SG_4 verwendet.

Die Schlüsselverteilzentrale SVZ bildet das Datenfeld DF aus einer Schlüsselkennung SK mit beispielsweise 128 Bits, aus zwei Schlüsselgerätekennungen GK_1 und GK_2 mit jeweils 24 Bits und aus zwei Schlüsselfeldern SF_1 und SF_2 mit jeweils 152 Bits. Die Schlüsselkennung SK ist derart aufgebaut, daß sie bei der normalen Übertragung von Nachrichten möglichst sehr selten vorkommt. Die Schlüsselgerätekennung GK_1 ist dem Schlüsselgerät SG_1 zugeordnet, und im Schlüsselfeld SF_1 ist der für das Schlüsselgerät SG_1 vorgesehene Schlüssel S_1 enthalten. Zusätzlich kann das Schlüsselfeld SF_1 Prüfzeichen P_1 für den Schlüssel S_1 und weitere Zeichen G_1 enthalten, die den Gültigkeitszeit-

punkt und/oder die Gültigkeitsdauer des Schlüssels S_1 festlegen. In entsprechender Weise ist die Schlüsselgerätekennung GK_2 dem Schlüsselgerät SG_2 zugeordnet, und das Schlüsselfeld SF_2 enthält den zugehörigen Schlüssel S_2 , sowie dessen Prüfzeichen P_2 und Zeichen G_2 für die Gültigkeit des Schlüssels S_2 . Die Schlüssel S_1 und S_2 umfassen beispielsweise jeweils 120 Bits, während die Prüfzeichen P_1 und P_2 16 Bits und die Zeichen G_1 und G_2 16 Bits umfassen. Die Schlüssel S_1 und S_2 sind vorteilhafterweise mit den Stationsschlüsseln der Schlüsselgeräte SG_1 bzw. SG_2 verschlüsselt.

Zu Beginn der Verteilung der Schlüssel S_1 und S_2 an die Schlüsselgeräte SG_1 und SG_2 stellt die Schlüsselverteilzentrale eine Verbindung zur Datenendeinrichtung DE_1 her, und überträgt den Datenblock über die Fernleitung FL_3 und FL_1 . Das Datenfeld DF wird dabei im Schlüsselgerät SG_5 verschlüsselt und im Schlüsselgerät SG_6 wieder entschlüsselt. Im Netzknoten NK liegt das Datenfeld unverschlüsselt vor, wobei jedoch die Schlüssel S_1 und S_2 , wie bereits erwähnt, mit den Stationsschlüsseln der Schlüsselgeräte SG_1 bzw. SG_2 verschlüsselt sind. Bei der verschlüsselten Übertragung des Datenfelds DF auf dem Streckenabschnitt zwischen dem Netzknoten NK und der Datenendeinrichtung DE_1 erkennen die Schlüsselgeräte SG_1 und SG_2 beim Empfang der Schlüsselkennung SK , daß im folgenden Schlüssel übertragen werden. Die Schlüsselgeräte SG_1 und SG_2 prüfen anschließend die Schlüsselgerätekennungen GK_1 und GK_2 . Wenn das Schlüsselgerät SG_1 die Schlüsselgerätekennung GK_1 erkennt, wird das im Datenfeld DF enthaltene Schlüsselfeld SF_1 in einen Speicher übernommen. In entsprechender Weise übernimmt das Schlüsselgerät SG_2 , wenn es die Schlüsselgerätekennung GK_2 als ihm zugeordnet erkennt, das Schlüsselfeld SF_2 in einen einen Speicher.

Weitere Einzelheiten werden im folgenden zusammen mit dem in Fig. 3 dargestellten Blockschaltbild beschrieben.

Bei dem in Fig. 3 dargestellten Blockschaltbild sind die für die Durchführung des Verfahrens erforderlichen Teile der Schlüsselgeräte SG_1 und SG_2 dargestellt. Es wird davon ausgegangen, daß über die Fernleitung FL_1 eine Halbduplexübertragung zwischen der Datenendeinrichtung DE_1 und dem Netzknoten NK erfolgt. Für eine Voll duplexübertragung müssen die entsprechenden Entschlüsselungs- und Verschlüsselungsstufen in den Schlüsselgeräten SG_1 und SG_2 in bekannter Weise nochmals vorhanden sein.

Wenn vom Netzknoten NK das Datenfeld DF unverschlüsselt abgegeben wird, erkennt eine Auswertestufe A_{21} im Schlüsselgerät SG_2 die Schlüsselkennung SK . Die Auswertestufe A_{21} gibt ein Steuersignal ST_2 an eine weitere Auswertestufe A_{22} , die im Datenfeld DF die Schlüsselgerätekennung GK_2 überprüft. Falls diese Schlüsselgerätekennung GK_2 dem Schlüsselgerät SG_2 zugeordnet ist, gibt sie ein Freigabesignal F_2 an einen Speicher SP_2 ab, in dem zumindest der Schlüssel S_2 und gegebenenfalls auch die Prüfzeichen P_2 und die Zeichen G_2 gespeichert werden. Die Prüfzeichen P_2 werden in einer Prüfstufe PS_2 ausgewertet. Falls die Prüfzeichen P_2 auf einen fehlerhaften Schlüssel S_2 hindeuten, wird dieser als ungültig erklärt. Die Prüfstufe PS_2 sorgt in diesem Fall für eine Trennung der Verbindung und gegebenenfalls für eine Mitteilung an die Schlüsselverteilzentrale SVZ . Die Zeichen G_2 können einer Zeitstufe Z_2 zugeführt werden, die den Gültigkeitszeitpunkt für den neuen

Schlüssel festlegt. Beim Eintritt des Gültigkeitszeitpunktes wird der Schlüssel S_2 vor oder nach einer Entschlüsselung mit dem, dem Schlüsselgerät SG_2 zugeordneten Stationsschlüssel der Schlüsselstufe VE_2 zugeführt. Es erfolgt in der Schlüsselstufe VE_2 die Entschlüsselung des Schlüssels S_2 .

Auf der Fernleitung FL_1 wird das Datenfeld DF verschlüsselt übertragen. Das Schlüsselgerät SG_1 enthält eine Schlüsselstufe VE_1 , die das Datenfeld DF entschlüsselt und der Datenendeinrichtung DE_1 zuführt. In ähnlicher Weise wie im Schlüsselgerät SG_2 ist im Schlüsselgerät SG_1 eine erste Auswertestufe A_{11} vorgesehen, die das Auftreten der Schlüsselkennung SK erkennt und ein Steuersignal ST_1 an eine weitere Auswertestufe A_{12} abgibt, die das Auftreten der Schlüsselgerätekennung GK_1 prüft. Wenn die Schlüsselgerätekennung GK_1 dem Schlüsselgerät SG_1 zugeordnet ist, gibt die Auswertestufe A_{12} ein Freigabesignal F_1 an einen Speicher SP_1 ab, um das Schlüsselfeld SF_1 einzuspeichern. Wenn eine Prüfstufe PS_1 die Richtigkeit des Schlüssels S_1 feststellt, wird dieser als gültig erklärt und die Zeichen G_1 können in einer Zeitstufe Z_1 eingespeichert werden, um den Gültigkeitszeitpunkt zu ermitteln. Wenn dieser eintritt, wird der Schlüssel S_1 , ebenfalls ver- oder entschlüsselt, der Schlüsselstufe VE_1 zugeführt. Die Prüfstufe PS_1 kann im Fall der Ungültigkeit des Schlüssels S_1 dies der Datenendeinrichtung DE_1 mitteilen oder selbst für eine Mitteilung an die Schlüsselverteizentrale SVZ sorgen und dann die Verbindung zum Netzknopen NK trennen. Datenübertragungsfehler werden im Rahmen der üblichen Datenübertragungsprozedur von Datenendeinrichtung DE erkannt, bewertet und gegebenenfalls wird eine Wiederholung der Übertragung veranlaßt.

Die Schlüssel S_1 und S_2 können in den Schlüsselstu-

fen VE_1 und VE_2 einem Verschlüssler und einem Entschlüssler zugeführt werden. Es ist auch möglich, für beide Übertragungseinrichtungen unterschiedliche Schlüssel zu verwenden. In diesem Fall müssen entweder zwei Datenblöcke übertragen werden, oder der Datenblock muß derart erweitert werden, daß in den Schlüsselfeldern SF_1 bzw. SF_2 auch die weiteren Schlüssel enthalten sind.

In ähnlicher Weise wie die Schlüssel den Schlüsselgeräten SG_1 und SG_2 zugewiesen werden, werden sie anschließend den Schlüsselgeräten SG_3 und SG_4 zugewiesen. In jedem Fall prüfen die Datenendeinrichtungen DE_1 und DE_2 durch übliche Prüfverfahren die Richtigkeit der empfangenen Datenblöcke. Nach der Verteilung der Schlüssel und nach dem Eintritt des Gültigkeitszeitpunktes kann mit der Übertragung der Daten zwischen den Datenendeinrichtungen DE_1 und DE_2 begonnen werden.

Bei einer Teilnehmer-Teilnehmer-Verschlüsselung sind die Datenübertragungseinheiten DU_2 , DU_3 und DU_6 und die Schlüsselgeräte SG_2 , SG_3 und SG_6 nicht erforderlich. In diesem Fall überträgt die Schlüsselverteizentrale SVZ an das Schlüsselgerät SG_1 ein Datenfeld, das nur die Schlüsselkennung SK , die Schlüsselgerätekennung GK_1 und das Schlüsselfeld SF_1 enthält. In entsprechender Weise wird an das Schlüsselgerät SG_4 ein Datenfeld DF übertragen, das nur die Schlüsselkennung SK , die Schlüsselgerätekennung GK_2 und das Schlüsselfeld SF_2 enthält. Um das gleiche Format des Datenfeldes DF beizubehalten, kann es dabei zweckmäßig sein, die nicht benötigte Schlüsselgerätekennung GK_1 und/oder das entsprechende Schlüsselfeld SF mit einer vereinbarten Adresse zu belegen.

Hierzu 1 Blatt Zeichnungen

FIG 1

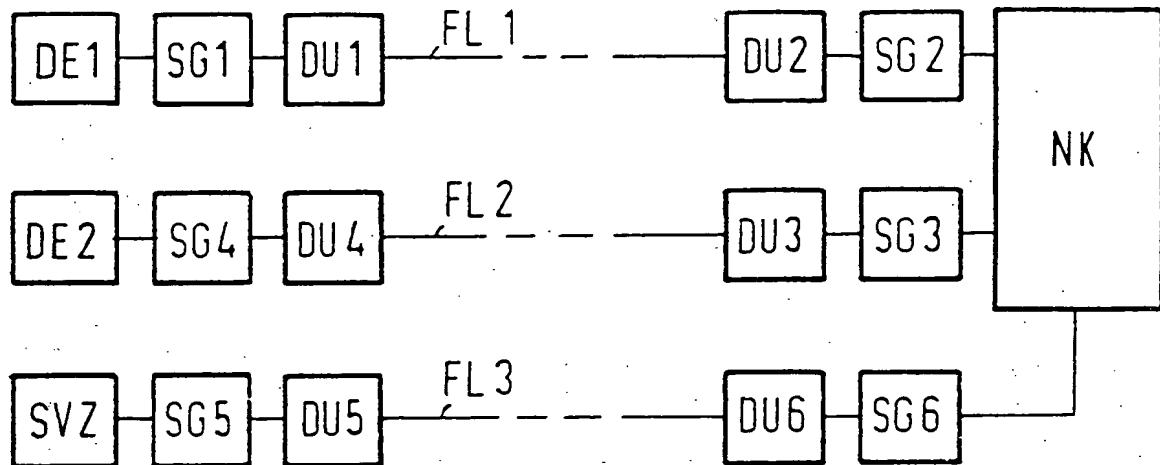


FIG 2

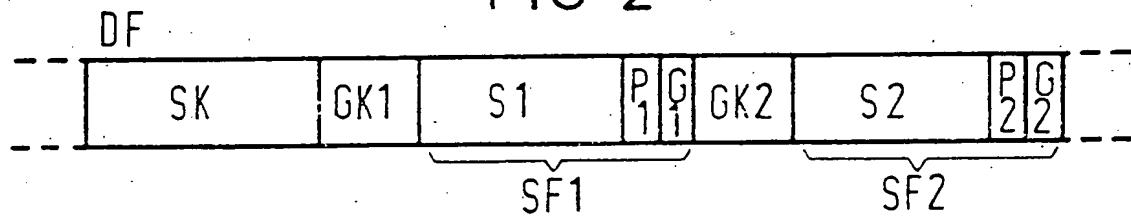


FIG 3

